UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/260,796	03/01/1999	JAMES P HUGHES	98-019-NSC	6934

7590 03/10/2003

TIMOTHY R SCHULTE
STORAGE TECHNOLOGY CORPORATION
2270 SOUTH 88TH STREET MS-4309
LOUISVILLE, CO 800284309

EXAMINER
DARROW, JUSTIN T

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 12

Application Number: 09/260,796
Filing Date: March 01, 1999
Appellant: HUGHES, JAMES P

Mark D. Chuey, Ph.D.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/31/2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1-5, 7, 9-11, 13, and 15-17 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

Group A: Claims 1 and 2.

Group B: Claims 9, 10, 13, 15-17.

Group C: Claim 11.

Group D: Claims 3-5.

Group E: Claim 7.

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

3,798,360 A	FEISTEL	6-1971
5,787,175 A	CARTER	7-1998

(10) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1, 2, 9, 11, 13, and 15-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Carter, U.S. Patent No. 5,787,175 A.

As per claim 1, Carter illustrates a method for secure handling of information comprising: authenticating a user group with a user group identifier and corresponding password (see column 8, lines 51-59; figure 2, item 48; column 12, lines 25-42; column 15, lines 63-67; column 16, lines 16-29 and 51-59; figure 4, items 90, 92, and 96; and figure 9, step 152); as a result of authentication, obtaining the private key of the user (see column 16, lines 30-37 and figure 9, step 154); and using the private key to decrypt the encrypted document key that is required to decrypt the document (see column 16, lines 60-65 and figure 9, step 160). Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4,

item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

As per claim 2, Carter embodies the functions of the operating system being incorporated in individual application programs to access documents (see column 9, lines 62-67; column 10, lines 1-2; figure 2, items 46, 48, 50, and 54; and figure 6, step 120).

As per claim 9, Carter describes a system for the secure handling of information comprising: a generator of public-key cryptographic keys which corresponds to the recited key manager (see column 8, lines 60-65; column 11, lines 55-67; and figure 3, item 74, 76, 78, and 80); an object database system with group objects and key objects which corresponds to the claimed at least one group server (see column 10, lines 14-20 and figure 3, items 70 and 74); a collaborative access controller which corresponds to the recited at least one producer client encrypting the data portion of a document which corresponds to the recited data set with a randomly generated document key which corresponds to the claimed encryption value (see column 13, lines 4-17; figure 2, item 50 and 54; figure 4, item 94; and figure 6, step 112); arranging collaborative group identification by identifying a group object or other group identifier (see column 13, lines 18-28; figure 2, item 48; figure 3, item 70; and figure 6, step 114); encrypting the document key with the public key of the collaborative group (see column 8, lines 60-67; column 11, lines 55-67; figure 3, items 74, 76, and 78; column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100); including the member group definition and an encrypted message digest containing the encrypted document key in the work group document (see column 12, lines 25-55; figure 4, items 54, 90, 94, and 96; and figure 5, items 96, 98, 100,

and 102); and storing the work group document in a file in a computer system (see column 12, lines 9-14 and figure 1, item 10).

As per claim 11, Carter points out that the member is verified if the corresponding identifier is found (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). Carter does not explicitly disclose the feature of a boolean combination resultant of true. However, this feature is deemed to be inherent to the system of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The system of Carter would be inoperative if this logical consequence did not result. Carter does not explicitly disclose the feature of an access formula. However, this feature is deemed to be inherent to the Carter method because the entered password would have to be compared with a stored value in order to determine granting user access (see column 16, lines 16-29; figure 4, item 90; figure 9, step 152). The Carter method would be inoperative if such a comparison were not made.

As per claim 13, Carter additionally show obtaining the private key (see column 16, lines 30-33; figure 9, step 154); determining that the document to which access is requested is a work group document (see column 16, lines 16-19; figure 2, item 54; and figure 4, item 90); searching the collaborative document for the member identifier (see column 16, lines 51-55 and figure 9, step 158); request access to the work group document (see column 16, lines 16-19 and figure 4, item 90); using the private key to decrypt the corresponding encrypted document key (see column 16, lines 60-65 and figure 9, step 160); and using the document key to decrypt the encrypted data portion of the collaborative document (see column 17, lines 5-10; figure 4, items 90 and 94; and figure 9, step 162).

As per claim 15, Carter further elaborates a user requesting the addition of a new member (see column 14, lines 44-51); verifying this user (see column 14, lines 44-51 and figure 7, step 122); decrypting the encrypted document key with the private key (see column 15, lines 17-23; figure 3, item 80; and figure 4, item 100); and encrypting the document key with the public key of the new member (see column 15, lines 22-23; figure 3, item 78; and figure 4, item 100).

As per claim 16, Carter suggests that the attempt to access the document is logged (see column 16, lines 44-50).

As per claim 17, Carter embodies the collaborative access controller operable to make changes including additions (see column 14, lines 44-51) and deletions (see column 15, lines 31-40).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3-5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carter, U.S. Patent No. 5,787,175 A in view of Feistel, U.S. Patent No. 3,798,360 A.

As per claim 3, Carter depicts a method for secure handling of information comprising: creating group objects (see column 10, lines 14-20 and figure 3, item 70); obtaining a public key and private key for each of the at least one group (see column 11, lines 61-67; column 12, lines

1-8; and figure 3, items 76, 78, and 80); encrypting the data portion of a document with a generated document key, preferably for use with a symmetric encryption method (see column 13, lines 4-17; figure 2, item 50 and 54; figure 3, items 68 and 70; figure 4, item 94; and figure 6, step 112); authentication of collaborative group by obtaining user identifiers (see column 13, lines 18-28; figure 2, item 48; and figure 6, item 114) which undergo validation (see column 13, lines 29-38) so that a group member or members can obtain the encrypted document key for accessing a document (see column 13, lines 63-67 and column 14, lines 1-5); encrypting the document key with the public key of the collaborative group (see column 13, lines 63-67; column 14, lines 1-5 and figure 5, item 100); including the member group definition containing the encrypted document key in the work group document (see column 12, lines 25-42; figure 4, items 54, 90, 94, and 96; and figure 5, item 100); and storing the work group document in a file in a computer system (see column 12, lines 9-14 and figure 1, item 10). Although Carter describes that the document key is preferably suitable for use with a symmetric cryptographic method (see column 13, lines 7-10), he does not explicitly teach that it is randomly generated. Feistel specifies a random key number generator in a symmetric key block cipher (see column 5, lines 18-23 and figure 1, item 43). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method for the secure handling of information of Carter with the random key generator of Feistel to have a degree of security that relates to the probability of guessing the unique combination of key binary digits by an opponent having both the knowledge of the internal circuitry of the system and the opportunity to observe prior transmissions and resulting ciphers (see column 5, lines 9-14).

As per claim 4, Carter further elaborates a user requesting the addition of a new member (see column 14, lines 44-51); verifying this user (see column 14, lines 44-51 and figure 7, step 122); decrypting the encrypted document key with the private key (see column 15, lines 17-23; figure 3, item 80; and figure 4, item 100); and encrypting the document key with the public key of the new member (see column 15, lines 22-23; figure 3, item 78; and figure 4, item 100).

As per claim 5, Carter suggests that the attempt to access the document is logged (see column 16, lines 44-50).

As per claim 7, Carter points out that the member is verified if the corresponding identifier is found (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). Carter does not explicitly disclose the feature of a boolean combination resultant of true. However, this feature is deemed to be inherent to the method of Carter as the finding of the member identifier in a logical alternative for access (see column 16, lines 51-62; column 15, lines 46-48; figure 5, item 98; and figure 9, step 154). The method of Carter would be inoperative if this logical consequence did not result.

5. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Carter, U.S. Patent No. 5,787,175 A in view of as applied to claim 9 above, and further in view of Feistel, U.S. Patent No. 3,798,360 A.

Carter discloses the system for the secure handling of information of claim 9. Although Carter describes that the document key is preferably suitable for use with a symmetric cryptographic method (see column 13, lines 7-10), he does not explicitly teach that it is randomly generated. Feistel specifies a random key number generator in a symmetric key block cipher (see column 5, lines 18-23 and figure 1, item 43). Therefore, it would have been obvious to one

of ordinary skill in the computer art at the time the invention was made to combine the system for the secure handling of information of Carter with the random key generator of Feistel to have a degree of security that relates to the probability of guessing the unique combination of key binary digits by an opponent having both the knowledge of the internal circuitry of the system and the opportunity to observe prior transmissions and resulting ciphers (see column 5, lines 9-14).

(11) Response to Argument

For the above reasons, it is believed that the rejections should be sustained.

Group A: Claims 1 and 2.

As per claim 1, Carter presents an authentication of a user in a user group to decrypt a key used in decrypting a workgroup document:

Carter describes a user identifier and password that is entered by the user.

Column 8, lines 51-59

> In some embodiments, the operating system 46 generates, maintains, and manages a set of user identifiers 48 such as login names or account numbers. User identifiers such as the identifiers 48 are commonly used to track resource use, to assist in verifying resource access rights, and to identify system users to one another. A login password is often, but not always, associated with each user identifier 48. Unless otherwise indicated, as used herein "password" includes both passwords and pass phrases.

Figure 2, item 48

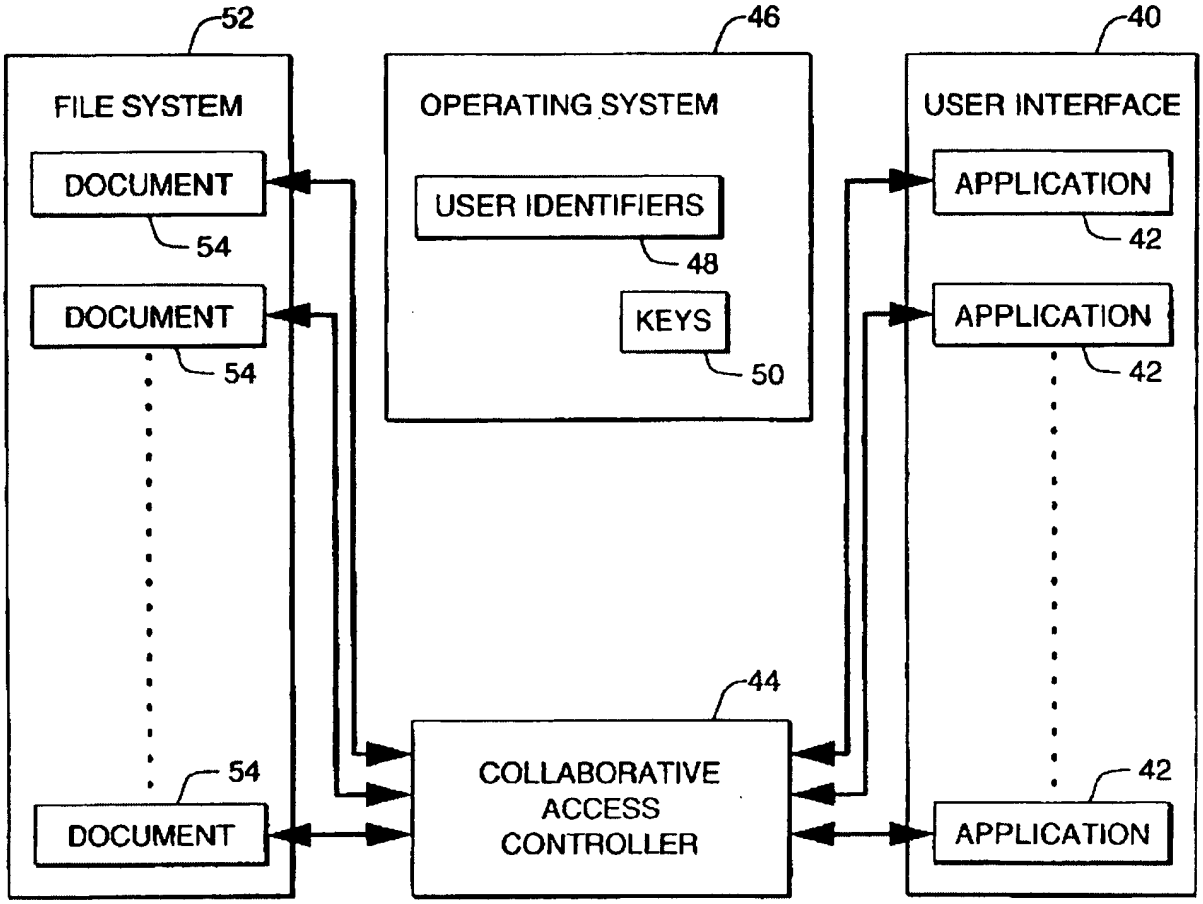

FIG. 2

Carter explains that the workgroup document contains member definitions of a collaborative group of users who have access to the data. This is a "group comprising a list of at least one client" as recited in claim 1. This is the access control list described by the appellant in the specification (see specification, page 15, lines 11-17 and figure 4)

Column 12, lines 25-42

With reference to FIGS. **4** and **5**, the prefix portion **92** of the work group document **90** includes at least one member definition **96**. The member definitions **96** may be located in the same file as the data portion **94** or in one or more separate files. As explained hereafter, the member definitions **96** define a collaborative group of computer system users which have access to the data portion **94** of the work group document **90**.

Each member definition **96** includes a member identifier **98**. Suitable member identifiers **98** include the user identifiers **48** (FIG. **2**) used by the operating system **46**, as well as identifiers defined exclusively for use in connection with work group document access according to the present invention. With reference to FIG. **3**, one or more members of the collaborative group may correspond to an individual user object **68**, to a group object **70**, or to an organizational role object **72** that is recognized by the network operating system **60**.

figure 4, items 90, 92, and 96

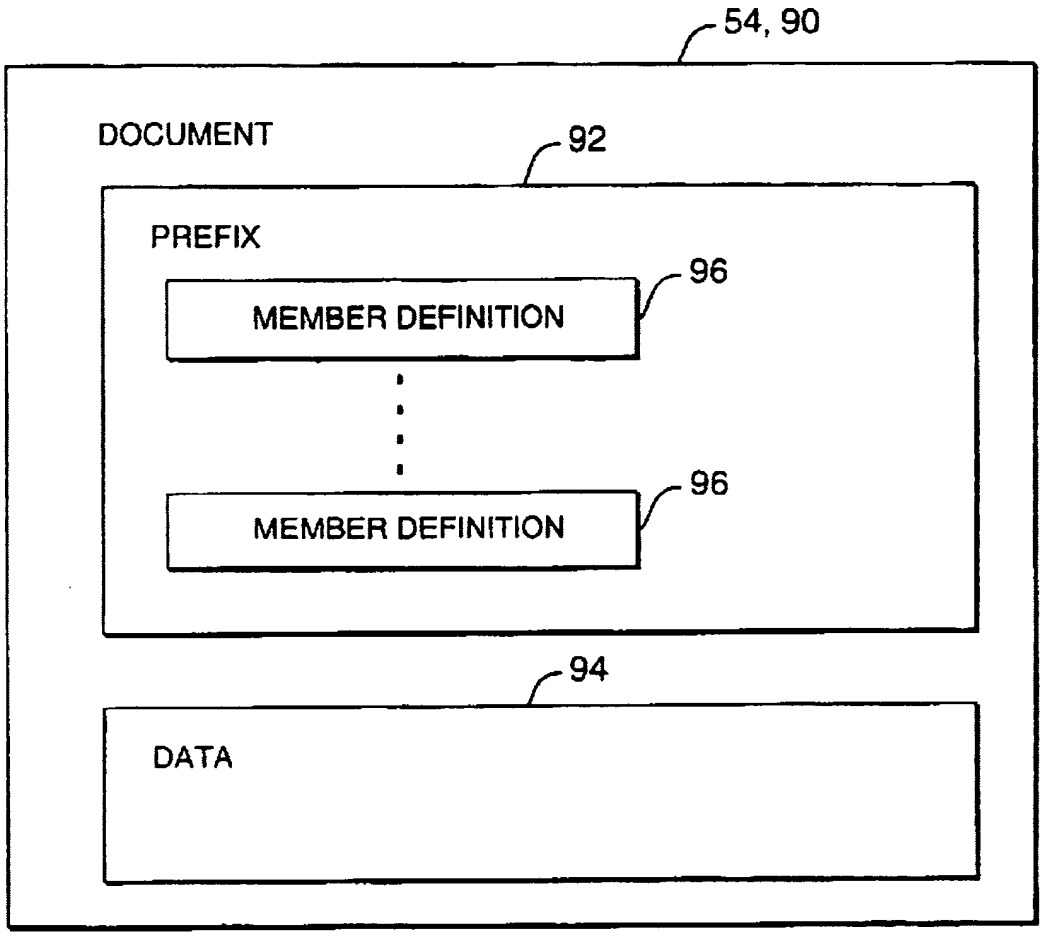

FIG. 4

Carter elaborates that the user inputs a user identifier and password; the member definitions of the collaborative document are searched in order to locate the member identifier corresponding to the user identifier.

Column 15, lines 63-67

FIGS. 2–6 and 9 illustrate a method according to the present invention for restricting access to the information in the data portion 94 of the work group document 90 so that members of the collaborative group have access and others do not. During a detecting step 150, the application 42

Column 16, lines 16-29

After it has been determined that the document 54 to which access is requested is a work group document 90, the obtaining step 152 is performed by the collaborative access controller 44. As with other portions of the collaborative access controller 44, the portion which performs the obtaining step 152 may be embodied within the application 52 or may be a separate module which is invoked by the application 52 or by the user. The obtaining step 152 comprises interactively asking the user for its user identifier and a corresponding password. In alternative embodiments, the user identifier identifies the current user and is obtained by querying the operating system 46 or the object database system 62; only the password is obtained interactively from the user.

Column 16, lines 51-59

If the key-seeking step 154 succeeds, a member-seeking step 158 is performed. The step 158 searches the member definitions 96 of the collaborative document 90 in an attempt to locate a member identifier 98 that corresponds to the user identifier obtained during the step 152. The search is accomplished substantially as described above in connection with the steps 122, 140, 142. If the search fails, then the user identifier does not identify a member of the collaborative group and the limiting step 156 is performed.

Figure 9, step 152

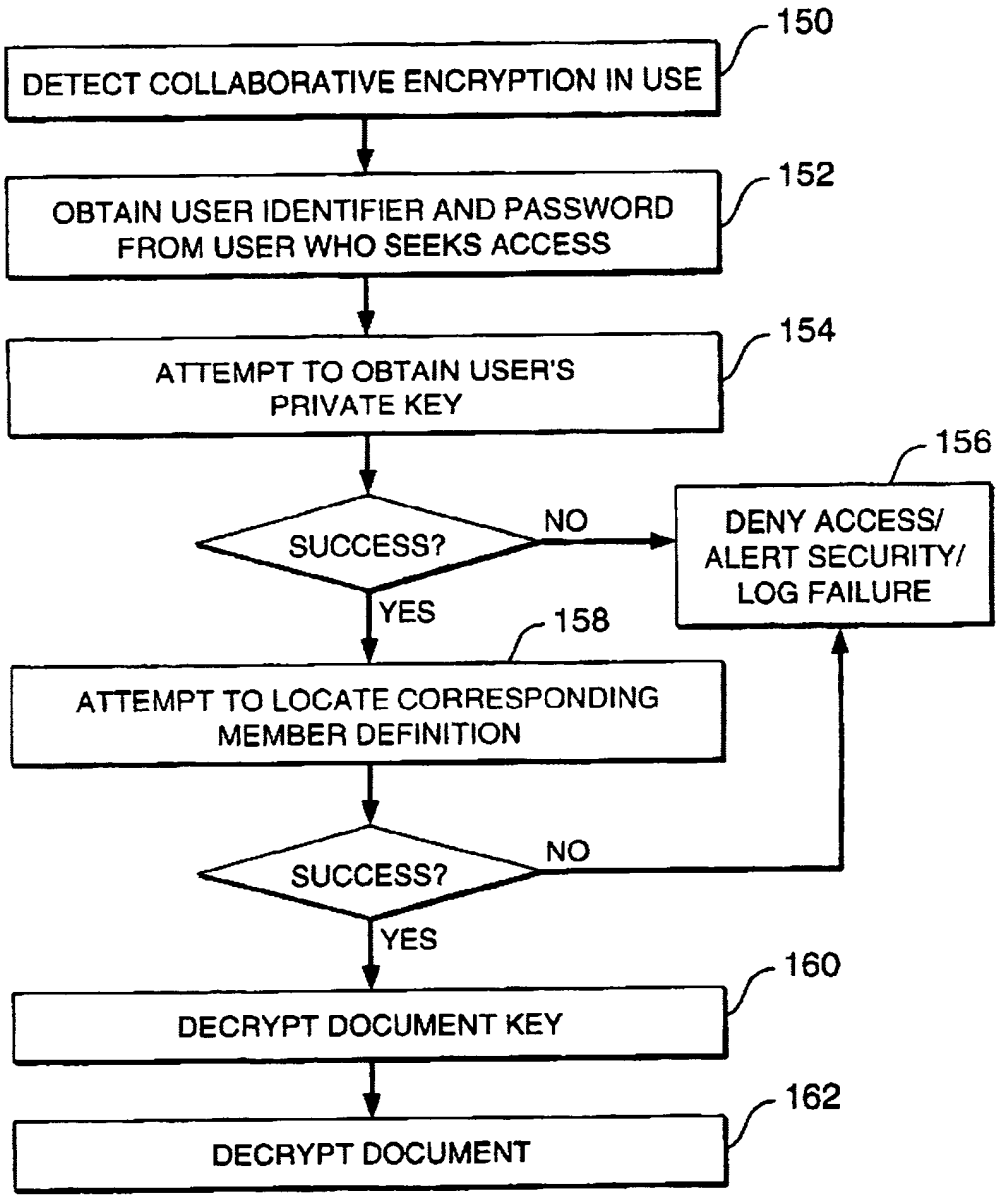

FIG. 9

It is clear that this search would require comparison to see that the member identifier, relating the member to the workgroup, is equal to the user identifier entered by the user to decrypt the

document key and decrypt the document. This is within the scope of "solving an access formula describing a function of groups, each group comprising a list of at least one client, wherein the requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula" explicitly recited in claim 1. This matching comparison is within the scope of an access formula as described by the appellant in the specification (see specification, page 10, lines 10-25 and figure 1, items 22 and 44). In Carter, the client is a member of M-of-N groups, where both M and N equal one. The appellant describes password entry to initiate the process of access to information in the specification (see specification, page 10, lines 27-30; page 11, lines 1-3; figure 1, item 22; figure 2, item 64; and figure 3, item 62).

Although Carter does not teach more complex formulas than a comparison does not mean that he teaches away from suggesting an access formula as recited in claim 1. There are possible reasons why Carter does not discuss values of M and N, each greater than one. Motivations for not requiring more complex access formulae is pointed out by Carter in terms of reducing lead times and expense (see column 2, lines 7-14). "A reference is no less anticipatory if, after disclosing the invention, the reference then disparages it. Thus, the question whether a reference "teaches away" from the invention is inapplicable to an anticipation analysis." *Celeritas Technologies Ltd. v. Rockwell International Corp.*, 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522 (Fed. Cir. 1998). See MPEP §§ 2123 and 2131.05.

A search that requires a comparison to see that the member identifier, relating the member to the workgroup, is equal to the user identifier entered by the user to decrypt the document key and decrypt the document is inherent because the method of Carter would be

inoperative. Because of this requirement, the access formula is necessarily present in the method of Carter for it to function and, thus, inherent. See *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

Group B: Claims 9, 10, 13, 15-17.

As per claim 9, Carter teaches a group server obtaining a private key and matched public key for each group:

Column 8, lines 60-67

Cryptographic Methods

In some embodiments, the operating system **46** also generates, maintains, and manages a set of keys **50**. Some of the keys **50** are generated by symmetric cryptographic methods while others are generated by public-key cryptographic methods. It is presently preferred to utilize encryption methods whose strength does not depend heavily on the

Column 11, lines 55-67

An NWAdmin snap-in module may be used to modify the directory services schema **66** to support key objects/attributes **74** according to the present invention. NWAdmin is a commercially available extendable tool used by network administrators to manage objects and attributes in object databases.

In some embodiments, key pairs **76** are stored in key objects **74**. In alternative embodiments, the key pairs **76** are stored in key attributes **74** which are then associated with user objects **68**, with group objects **70**, and/or with organizational role objects **72**. Those of skill in the art will readily determine appropriate storage locations for the key pairs **76**

Figure 3, items 74, 76, 78

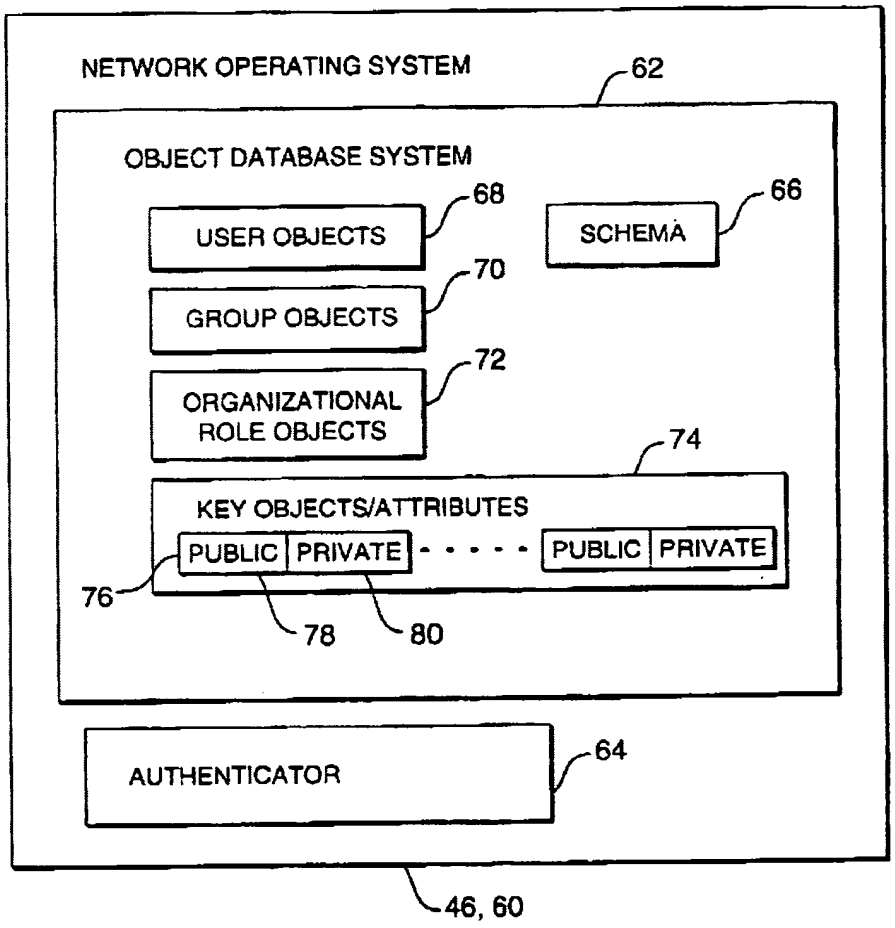
NETWORK OPERATING SYSTEM
62
OBJECT DATABASE SYSTEM
USER OBJECTS
68
SCHEMA
66
GROUP OBJECTS
70
ORGANIZATIONAL ROLE OBJECTS
72
74
KEY OBJECTS/ATTRIBUTES
PUBLIC
PRIVATE
PUBLIC
PRIVATE
76
78
80
AUTHENTICATOR
64
46, 60

FIG. 3

Carter points out that the public key pairs are associated with the groups, not just with individual members of the groups. As pointed out in the response to arguments for Group A, these keys are used in decrypting the symmetric key used to decrypt the workgroup document.

Group C: Claim 11.

As per claim 11, Carter discloses that the search results in one of either of two alternatives, failure or success. This is equivalent to the Boolean results of true or false. This feature is inherent to the system of Carter. The system of Carter would not function if this logical consequence did not result.

Column 16, lines 51-61

If the key-seeking step **154** succeeds, a member-seeking step **158** is performed. The step **158** searches the member definitions **96** of the collaborative document **90** in an attempt to locate a member identifier **98** that corresponds to the user identifier obtained during the step **152**. The search is accomplished substantially as described above in connection with the steps **122**, **140**, **142**. If the search fails, then the user identifier does not identify a member of the collaborative group and the limiting step **156** is performed.

If the search succeeds, a key-decrypting step **160** is performed. The private key **80** obtained during the step **154**

Group D: Claims 3-5.

As per claim 3, Carter does teach acquiring a public key and matched private key for each of the at least one group. This step is pointed out in the response to argument for Group B. Carter also suggests the formula for gaining access. This feature is discussed above in response to the argument for Group A.

Group E: Claim 7.

As per claim 7, Carter discloses that the search results in one of either of two alternatives, failure or success. As pointed out above in the response to argument for Group C, this is equivalent to the Boolean results of true or false. This feature is inherent to the system of Carter. The system of Carter would not function if this logical consequence did not result.

(12) Conclusion

The appellant has not distinguished the invention of claims 1-5, 7, 9-11, 13, and 15-17 over the prior art of record. Therefore, for the above reasons, the rejections should be maintained.

Respectfully submitted,

JUSTIN T. DARROW
PRIMARY EXAMINER

March 9, 2003

Conferees

GB Gilberto Barron Jr.
SPE 2132

MS
Matthew Smithers
Primary Examiner
Art Unit 2134

TIMOTHY R SCHULTE
STORAGE TECHNOLOGY CORPORATION
2270 SOUTH 88TH STREET MS-4309
LOUISVILLE, CO 80028-4309